U.S. FISH AND WILDLIFE SERVICE TRANSMITTAL SHEET

PART 270 FW 1, 2, 4, 6, 7 & 8	SUBJECT ITM Program Management	RELEASE NO. 406
FOR FURTHER INFORMATION CONTACT Division of Information Technology Management		DATE September 30, 2002

EXPLANATION OF MATERIAL TRANSMITTED:

270 FW 1 describes the Fish and Wildlife Service Information Technology Architecture (SITA).

270 FW 2 defines policies for planning and managing investments in information technology and automated information systems.

270 FW 4 establishes policies and procedures for performing management control reviews of automated information systems in the Service.

270 FW 6 defines data management practices and the process for establishing data standards.

270 FW 7 identifies the policies, procedures, and responsibilities that form the basis of the Service's automated information technology (IT) security program.

270 FW 8 states the objectives of the spatial data management program.

Marshall P Jones Jr

Deputy DIRECTOR

FILING INSTRUCTIONS:

Remove:

270 FW 3, 03/08/94, FWM 130 (5 pages)
270 FW 4, 03/08/94, FWM 130 (4 pages)
Illustration 1, 270 FW 4, 03/08/94, FWM 130 (1 page)
Illustration 2, 270 FW 4, 03/08/94, FWM 130 (1 page)
270 FW 7, 10/13/92, FWM 042 (4 pages)
Exhibit 1, 270 FW 7, 10/13/92, FWM 042 (2 pages)
Appendix 1, 270 FW 7, 10/13/92, FWM 042 (3 pages)
Appendix 2, 270 FW 7, 10/13/92, FWM 042 (1 page)
Appendix 3, 270 FW 7, 10/13/92, FWM 042 (2 pages)

Insert:

270 FW 1, 09/30/02, FWM 406 (2 pages)
270 FW 2, 09/30/02, FWM 406 (5 pages)
270 FW 4, 09/30/02, FWM 406 (4 pages)
270 FW 6, 09/30/02, FWM 406 (3 pages)
270 FW 7, 09/30/02, FWM 406 (6 pages)
Exhibit 1, 270 FW 7, 09/30/02, FWM 406 (4 pages)
Exhibit 2, 270 FW 7, 09/30/02, FWM 406 (2 pages)
Exhibit 3, 270 FW 7, 09/30/02, FWM 406 (2 pages)
Exhibit 4, 270 FW 7, 09/30/02, FWM 406 (4 pages)
270 FW 8, 09/30/02, FWM 406 (3 pages)

Chapter 7 Automated Information System Security 270 FW 7

7.1 What is the purpose of this chapter? This chapter identifies the policies, procedures, and responsibilities that form the basis of the Service's automated information technology (IT) security program, which is designed to ensure an appropriate level of security for Service automated information systems and associated data and resources. The goal is to protect the Service's investment in systems, data and associated resources from loss, unauthorized disclosure, alteration, or destruction and to inform Service employees of their responsibilities to safeguard Service data and IT. This chapter does not apply to the deployment and support of Departmentally mandated systems.

7.2 Why do we have an IT security program? Several statutes and Federal and Departmental policies mandate the establishment of an IT security program in the Service.

A. The Office of Management and Budget (OMB) Circular Number A-130, Management of Federal Information Resources, Appendix III.

B. The Computer Security Act of 1987, Pub. L. 100-235.

C. Information Technology Management Reform Act of 1996 (Clinger-Cohen Act).

D. Government Information Security Reform Act of 2000.

E. 375 DM 19.

F. Department of the Interior's Information Technology Security Plan.

7.3 What is the Service's policy on IT security?

A. Every major application and general support system (GSS) must have a system security plan documenting that all appropriate security controls have been considered, addressed, implemented, and tested. System security plans should follow the guidance and format in Exhibit 1. System security plans are recommended for other systems as well.

B. Every major application and GSS will have documented user account policies and procedures (see paragraph 7.4).

C. Every major application and GSS will provide controls commensurate with the levels of access granted to system users and administrators (paragraph 7.5).

D. All local and wide area networks will be managed and documented as a GSS (paragraph 7.6).

E. Personal computers at an installation will be managed and documented as components of the installation's network or otherwise as components of a single GSS with appropriate protection and security. PC security will comply with the guidelines in Exhibit 2.

F. All system users will receive IT security awareness training appropriate to their level of access (paragraph 7.7).

G. All systems will conform to the security architecture requirements as identified in the Service Information and Technology Architecture (SITA) (see 270 FW 1).

H. Service employees with IT duties will have risk level designations and position sensitivity designations detailed in 430 FW 1.

I. All threats to IT in the Service will be promptly reported, processed, and documented in accordance with standard incident response procedures on the Service's IT security page on the Intranet.

J. Any Service server that is accessible to the public over the Internet, such as web servers and application servers that provide information or services to the public, will be documented as a GSS and registered in accordance with procedures described in SITA.

7.4 What is the Service's process for managing user accounts? There are four elements that must be addressed when managing accounts:

A. Statement of Responsibility. Each supervisor is responsible for ensuring that their employees, contract personnel, and any other category of personnel requiring access to Service systems for the performance of their duties complete FWS Form 3-2212 (Automated Information System Statement of Responsibility) (SOR) prior to gaining access to any Service computer, terminal, network, or system. The supervisor should retain a copy of FWS Form 3-2212 and provide a copy to the user's Installation IT Security Manager (IITSM). The employee should retain the original SOR. Only one such statement per user is required regardless of the number of systems accessed.

B. Application for user account. If a system requires user authentication to gain access, the system owner must formulate and implement an application process to validate users that access the system. The process should include an application form that identifies the employee, the reason for access, and the level of access required. The application should require a copy of a valid SOR and a signed FWS Form 3-2211 (Password Control Document). The application should be signed by the employee's supervisor. Upon approval of the application, the system owner will provide a copy of the password control document to the user's IITSM.

C. Review and re-validation of user accounts. The system owner should provide for an annual review and validation of the access rights and requirements for all users with access to the system. The user's supervisor should sign a renewal line on the application (see subparagraph B, above) and indicate if changes to the type of system access are needed. All changes should be provided to the user's IITSM.

D. Termination of user accounts. When access to a system is no longer required, including transfer or departure of an employee, the supervisor will notify the IITSM, who will in turn notify the system owner of each system for which that employee has a system application on file. System owners and IITSMs will enter the date access was removed and retain the information for 1 year.

7.5 What are the Service's requirements for access controls? Every system that provides access to information will identify the levels of access required and implement corresponding access controls to ensure that every user has the appropriate level of access, that every account is assigned to a single individual, and that accounts are not used by others. Security requirements should be based on criteria such as sensitivity of the information, levels of access, and internal or external client access needs. A system that requires any kind of restricted access rights will assign unique IDs and passwords to each user according to the standards in Exhibit 3.

7.6 What are the Service's network security requirements? Service organizations increasingly rely on local and wide area networks to provide access to automated information systems, and this general support function brings with it increased potential for damage. More in depth information on network security can be found in the Network Architecture section of the SITA.

A. Network managers will prepare system security plans, document access control policies and procedures, and document their password controls in compliance with paragraphs 7.3A, B, and C.

B. All networked systems must display a warning message at login which can be found on the Service's IT security page on the Intranet.

C. Circuits will not be connected to modems in any device (such as personal computers, laptop computers, servers, fax machines) without explicit approval by the local IITSM and network manager. Modems that are approved for connection are prohibited from being set in a host mode that allows dialup access without explicit approval from the local IITSM and network manager.

D. A network should be used only for official business and activities within the guidelines of the Service's IT Appropriate Use policy on the Service's IT security page on the Intranet.

E. Network operating systems and system software must be documented as part of configuration management and change control procedures for all local and wide area networks.

F. Network administrators are the only ones authorized to store executable software on network servers, and no shareware, freeware, or public domain software will be used on any part of a network without the network administrator's approval.

G. Users will not copy commercial software that is resident on a network to a local computer without permission of the network administrator. Commercially developed software is proprietary and protected under copyright law.

H. Use of the network for backup purposes will be in compliance with procedures established by the network administrator. Use of the Service Wide Area Network (SWAN) for backups requires approval from the SWAN administrator in the National Communications Center (NCC) in the Division of Information Technology Management - Washington Office (ITM-WO).

I. Networks servers must be backed up. At least one full system backup must be performed weekly, and incremental backups performed on a regular established schedule. Backup media should be kept for a minimum of 30 days.

J. All Service local area networks require the use of a unique user ID and password for user access to the system.

K. All firewall plans must comply with the Service's perimeter security plan (managed by the NCC) and be reviewed and approved by NCC prior to implementation.

L. All intrusion detection plans must be reviewed and coordinated with the NCC prior to implementation and comply with pertinent SITA standards.

M. Establishment of new connections (direct or indirect) to the SWAN must be coordinated with the Regional ITM office and approved by the NCC prior to implementation.

7.7 What should IT security awareness training cover? All system users are required by the Computer Security Act of 1987 and OMB Circular A-130, Appendix III, to receive security awareness training appropriate to their level of access. Users of GSS and major applications are required to have additional security training specific to the access and operation of those systems and/or applications. The BITSM will provide guidance to systems and offices on appropriate security training.

A. Security awareness training for users should stress the Service's acceptable use and best practice policies, email privacy, user responsibility, and incident reporting. The training should provide the knowledge and skills needed to apply these elements in day-to-day computing.

B. Security awareness training for managers should include the elements from the user training, but emphasize management security responsibilities, how to handle reported incidents, and incorporating security into program operations.

C. System-specific security training for GSS and major applications is the responsibility of the system owner. System/application security training should be based on the Service security policies, and at a minimum should identify proper access and exiting of the system, and password requirements. Users must also be aware of the sensitivity of the information they process, and know how and to whom to report a security incident.

D. Training is a continuous process and at a minimum should be provided whenever there is a significant change in the organization's information security environment or procedures. All new employees must be provided adequate training at the time of employment and refresher training should be provided to all employees on an annual basis.

7.8 Where can I find more information on IT security? The Service's IT security page on the Intranet is maintained by the Bureau IT Security Manager (BITSM). It covers many areas addressed in this chapter in greater detail, as well as providing additional guidance for computer security management and generally accepted security practices.

7.9 Who is responsible for implementing the provisions of this chapter?

A. The **Director** provides the high-level visibility and support required to implement and maintain a viable and effective IT Security Program.

B. Assistant Directors and Regional Directors are responsible for ensuring that their staffs implement these policies and procedures.

C. The **Chief Technology Officer (CTO)** has oversight responsibility for the Service's IT security program and has responsibility for ensuring that appropriate IT Security is implemented and enforced within the headquarters office. The CTO designates the Service's BITSM. The CTO will appoint the IITSM for Headquarters office.

D. Regional Directors have responsibility for:

(1) Ensuring that appropriate IT Security is implemented and enforced within their Regions.

(2) Appointing the IITSM and an alternate for their installations. All appointments will be in writing and a copy of the appointment document forwarded to the BITSM.

(3) Ensuring that IITSMs are knowledgeable about IT, are capable of serving as an IT security resource for the installation, do not report to anyone responsible for system design or development, and annually receive appropriate security-related training to maintain proficiency.

E. Automated Information System Owners are responsible for:

(1) Funding, implementing, reviewing and enforcing all aspects of IT system security for their systems.

(2) Ensuring that the costs of security controls are explicitly identified as part of the life cycle planning of the overall system.

(3) Assigning a system security manager who is knowledgeable about IT security, Service IT security policies, and all aspects of the system's security.

(4) Ensuring that adequate security requirements are incorporated into system or contract specifications prior to the acquisition or design of these systems.

(5) Providing system accreditation documentation for any new major application or GSS to ITM-WO that authorizes in writing the use of the system and certifies that it has a written, tested, and implemented security plan per paragraph 7.3A and Exhibit 1 which adequately protects the system and its data. The system must be authorized prior to implementation. Authorization implies accepting identified risks of the system and certifying that the system satisfies applicable IT security policies, regulations, and standards, and that its security safeguards are adequate. The format for system accreditation can be found in 270 FW 2.

F. System Security Managers are responsible for all IT security aspects of the system and will ensure that the following controls are in place:

(1) Formulation, implementation, and maintenance of a system security plan for their major applications and GSS consistent with Service and Departmental guidance (paragraph 7.3A and Exhibit 1).

(2) Ensuring that the system incorporates SITA security controls and architecture.

(3) Performing periodic independent reviews or audits of security controls in the system security plan at least every 3 years, or when significant changes are made to the system, using information obtained from risk assessments, audits and reviews. See 270 FW 4 and NIST Special Publication 800-26 for further information.

(4) Ensuring that adequate physical and administrative safeguards are operational.

(5) Ensuring that the type and range of system access to information and data is restricted to authorized personnel on a need-to-know basis.

G. The Bureau IT Security Manager (BITSM) is responsible for:

(1) Developing the Service's IT Security Program by clarifying and adapting laws, regulations, Departmental guidelines, best practices, etc. to the specific needs of the Service.

(2) Maintaining and updating the Security Architecture component of SITA.

(3) Coordinating security policy and technical controls with Regional CTOs, IITSMs and system security managers.

(4) Issuing security policies, handbooks, guidance, and bulletins to keep Service managers, employees, and contractors informed about the security program and their responsibilities.

(5) Developing, implementing, and maintaining a Servicewide IT security training program that provides for mandatory periodic training in computer security awareness and acceptable practice. Ensures that training requirements are met and documented.

(6) Providing assistance with IT security at individual Regions and offices.

(7) Preparing reports, status documents, and briefings concerning the IT Security Program as requested by Service management or as required by law or other mandates.

(8) Serving as primary point of contact with the Department's IT Security Manager and incident response team.

(9) Coordinating with servicing personnel officers to set policy on the appropriate risk/sensitivity level and screening requirements for positions with IT responsibilities.

H. The National Network Security Manager (NNSM) is responsible for:

(1) Managing the Service's network security program including the design and implementation of technical solutions for the protection of SWAN resources, including perimeter security and intrusion detection.

(2) Incorporating technical security controls into the Security Architecture and Network Architecture components of the SITA.

(3) Coordinating network security controls and policies with Regional CTOs, IITSMs and system security managers.

(4) Providing assistance with network security at individual Regions and offices.

(5) Preparing reports, status documents, and briefings concerning the network security program as requested by Service management or as required by law or other mandates.

(6) Serving as secondary point of contact with the Department's IT Security Manager and incident response team.

(7) Serving as the alternate point of contact to the BITSM.

I. Installation IT Security Managers (IITSM) are responsible for:

(1) Serving as primary point of contact for security-related issues within their Region or installation and reporting security incidents to the BITSM.

(2) Assisting system owners identify and assess risk, explore controls and countermeasures, and implement approved IT security policies and procedures.

(3) Assisting with IT security safeguards included in contract specifications for the acquisition or operation of hardware, software development, or equipment maintenance services for the installation.

(4) Developing procedures and guidance necessary for the implementation of an appropriate security program.

(5) Investigating, documenting, and reporting any actual or perceived violation of security and alerting the BITSM of violations with potential for impact beyond the IITSM's area of control.

(6) Identifying security-related training requirements for all system users and recommending appropriate techniques or programs to management.

(7) Documenting users who have taken mandatory security training and providing this information to the BITSM.

(8) Conducting the risk assessment, identifying physical vulnerabilities, and recommending cost effective countermeasures appropriate for the site's facility, including computer rooms and other environments hosting data processing equipment. See Exhibit 4 for more information.

(9) Documenting networks and personal computers at their installations as one or more GSS.

(10) Documenting circuits at their installation that have been approved for connection to modems in devices such as personal computers, laptop computers, servers, fax machines, and documenting modems that are approved for being set in a host mode that allows dialup access.

(11) Coordinating with servicing personnel officers to ensure that positions with IT duties have the appropriate risk/sensitivity level assigned and that appropriate screening is conducted where applicable.

(12) Ensuring that PC security complies with the guidelines in Exhibit 2.

J. Managers and Supervisors whose staff use IT are responsible for:

(1) Ensuring that all users under their supervision are knowledgeable of and adhere to the security policies and procedures that implement the requirements of this chapter.

(2) Promptly reporting to the IITSM any incident that may indicate a violation of those policies and procedures.

(3) Ensuring that their employees, contract personnel, and any other category of personnel requiring regular access to Service systems for the performance of their duties read the Service's IT Appropriate Use Policy and complete FWS Form 3-2212 (paragraph 7.4A) prior to gaining access to systems.

(4) Reporting to the IITSM any change in employment status (such as transfer or termination) that necessitates removal from the system or change in the user's accounts.

(5) Coordinating with the IITSM to ensure that employees receive required IT security awareness training.

(6) Coordinating with IITSMs to develop employee job descriptions and performance standards which contain appropriate references to their IT security responsibilities and to ensure that employees receive security clearances and access levels appropriate to the job they will perform.

K. System End-Users are responsible for:

(1) Adhering to the security procedures implemented by their supervisors and the IITSM.

(2) Reporting to their supervisor or IITSM any condition or event that might represent a possible breach of system security.

(3) Taking IT security training mandated by the Service's IT security training program.

7.10 What special terms do I need to know?

A. Bureau IT Security Manager (BITSM). Person responsible for the Service's information resources security program.

B. Chief Technology Officer (CTO). Official who is responsible for coordinating IT issues on a Servicewide basis and for ensuring that information resources support the Service's strategic missions. The CTO is the Chief of the Division of Information Technology Management - Washington Office.

C. General Support System (GSS). Term from OMB Circular A-130, Appendix III, meaning an interconnected set of information resources under the same direct management control which shares common functionality and normally includes hardware, software, information, data, applications, communications, and people. Examples are local and wide area networks, telecommunications systems, and electronic mail systems.

D. Automated Information System. A discrete set of information and IT organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Automated information systems include both general support systems and major applications as those terms are defined in OMB Circular A-130, Appendix III. Examples are local and wide area networks, telecommunications systems, electronic mail systems, geographic information system (GIS) projects, data creation projects, databases, and radio projects.

E. Automated Information System Owner. The senior manager having overall functional responsibility for the program or activity in which a specific automated information system is conceived, planned, funded, developed, acquired, operated and maintained.

F. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Typically, IT includes hardware and software pertaining to computers, telecommunications, networks, and radio equipment.

G. IT Security. The combination of physical, administrative, and technical measures applied to protect the IT assets from loss, destruction, misuse, alteration, unauthorized disclosure, or access.

H. Installation IT Security Managers (IITSM). Officials at IT installations who are responsible for IT security at their facilities. Regions have discretion in assigning IITSMs as long as appropriate separation of duties and accountability is maintained.

I. Major Application. Term from OMB Circular A-130, Appendix III, meaning an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Do not confuse this term with the term "major automated information system" that is used in 270 FW 2, OMB Circular A-11, and the body of A-130 to designate certain levels of capital investment for a system.

J. National Network Security Manager (NNSM). Manages the Service's network security program including the design and implementation of technical solutions for the protection of SWAN resources.

K. Regional CTO. The person designated by each Region to coordinate IT issues between that Region and the ITM-WO.

L. Service Information and Technology Architecture (SITA). The set of Service standards, policies, and procedures that align data and IT with the Service's mission and goals and guide automated information system owners and developers so they know the IT infrastructure that is supported in the Service. See 270 FW 1.

M. System Security Managers. Appointed by system owners and are responsible for all IT security aspects of the system.